UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

JOSHUA ADAM SCHULTE,

Defendant.

17 Cr. 548 (PAC)

OPINION & ORDER

HONORABLE PAUL A. CROTTY, United States District Judge:

From March to November 2017, the website WikiLeaks made a series of disclosures of source code and documents (the "Leaks") relating to cyber tools developed by the Central Intelligence Agency ("CIA"). The Government has charged Joshua Schulte, a former CIA employee, with stealing and leaking national defense information, along with other charges, which include possession of child pornography and copyright infringement. (Dkt. 68.)

The Government has moved *ex parte* pursuant to Section 4 of the Classified Information Procedures Act, 18 U.S.C. APP. 3 ("CIPA") and Fed. R. Crim. P. 16(d)(1) for a protective order so that the Government need not produce certain materials that contain classified information. Pursuant to CIPA, the Government did not submit its motion to Schulte. The Government did, however, notify defense counsel that it made a classified *ex parte* submission to the Court on December 10, 2018.

The Government has produced a large volume of classified discovery to Schulte, and his defense counsel who have obtained the necessary security clearances, pursuant to the procedures outlined in CIPA. Under CIPA § 4 and Fed. R. Crim. P. 16(d)(1), the Government has also withheld some discovery on the basis that it is not discoverable and/or that the state-secrets

privilege applies to the data and its disclosure to Schulte is not required under CIPA, since it would not be helpful or material to his defense. This withheld information includes specific documents (see *infra* Section II.A), email communications (see *infra* Section II.B), and forensic evidence (see *infra* Section II.C).

Over the past several months, the Court has reviewed the Government's CIPA § 4 briefing, specific documents that were withheld, and the methodology used for withholding forensic data from discovery. The Court held *ex parte* hearings with the Government to discuss the CIPA § 4 motion, met *ex parte* with defense counsel to learn about Schulte's defense and discovery needs, heard from both parties in joint discovery conferences, and reviewed written submissions from both parties detailing discovery disputes. In considering all of this information, the Court placed itself "in the shoes of defense counsel, the very ones that cannot see the classified record," to determine whether the withheld data might be relevant and helpful to the defense. *United States v. Amawi*, 695 F.3d 457, 471 (6th Cir. 2012).

Based on this full review and for the following reasons, the Government is directed to disclose certain additional information to defense counsel; the remainder of the Government's motion is granted.

DISCUSSION

I. Legal Standards

A. Rule 16

Fed. R. Crim. P. 16 governs pretrial discovery in criminal matters. Documents and objects in the government's control are discoverable if (1) they are "material to preparing the defense," (2) "the government intends to use [them] in its case-in-chief at trial," or (3) they were "obtained from or belong[] to the defendant." Fed. R. Crim. P. 16(a)(E).

"Discoverable" information in the CIPA context includes "what should be made available in pretrial discovery, as well as exculpatory facts, or information relevant to the credibility of government witnesses, that need not be disclosed before trial but nonetheless must be made available in time for effective use at trial." *United States v. Rahman*, 870 F. Supp. 47, 50 (S.D.N.Y. 1994).

B. CIPA Standard

CIPA provides for the protection of classified information in criminal cases. The statute is "meant to protect and restrict the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *United States v. Aref*, 533 F.3d 72, 78 (2d Cir. 2008) (alterations and internal quotation marks omitted). "The Second Circuit has found that the governmental privilege contemplated under CIPA has its origins in the state secrets privilege, which 'allows the government to withhold information from discovery when that disclosure would be inimical to national security.'" *United States v. Ng Lap Seng*, No. S5 15-CR-706 (VSB), 2017 WL 2693625, at *2 (S.D.N.Y. June 21, 2017) (quoting *United States v. Abu-Jihaad*, 630 F.3d 102, 139-40 (2d Cir. 2010)).

Where classified information is implicated in criminal discovery, the government may make an *ex parte* motion to "delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove." 18 U.S.C. APP. 3 § 4.

"In a case involving classified documents . . . *ex parte, in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that

the district court may use in order to decide the relevancy of the information." *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998). Such hearings are appropriate "if the court has questions about the confidential nature of the information or its relevancy." *Id.* *Ex parte* hearings with the Government regarding CIPA § 4 submissions are standard practice in this district when cases involve discovery of classified information, even where defense counsel has secured security clearances. *See, e.g.*, *United States v. al-Kassar*, 07 Cr. 354 (JSR) (2009); *United States v. Kassir*, S2 04 Cr. 356 (JFK) (2008). To better understand the discovery needs of defendants in considering CIPA § 4 motions, courts sometimes hold *ex parte* conferences with or request *ex parte* submissions from defense counsel. *See Kassir*, S2 04 Cr. 356 (JFK) (2008).

As a threshold matter, a CIPA § 4 motion must establish that the information at issue is indeed classified. Classified information is "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))." 18 U.S.C. APP. 3 § 1(a). National security is "the national defense and foreign relations of the United States." 18 U.S.C. APP. 3 § 1(b).

The Second Circuit follows a three-part test in deciding whether a sufficient showing under 18 U.S.C. APP. 3 § 4 has been made, such that the state secrets privilege overrides a defendant's right to prepare a defense:

(1) whether the material in dispute is discoverable under Rule 16;

(2) whether the state-secrets privilege applies, because (a) "there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national

security, should not be divulged" and (b) "the privilege is lodged by the head of the department which has control over the matter, after actual personal consideration by that officer"; and

(3) whether the material is helpful or material to the defense, which need not rise to the level of exculpatory information contemplated by *Brady*. *See Aref*, 533 F.3d at 80.

If the court finds that the information is discoverable and helpful or material to the defense, the court then must decide whether the information should be disclosed and the form in which it should be disclosed. If the information is relevant or helpful, the court must balance the "public interest in protecting the flow of information against the individual's right to prepare his defense." *United States v. Mostafa*, 992 F. Supp. 2d 335, 338 (S.D.N.Y. 2014) (quoting *Roviaro v. United States*, 353 U.S. 53, 62 (1957)). When determining whether discoverable, helpful, and material classified material should be disclosed to the defense, "the test to be applied involves balancing the defendant's need for the information or its value to the defendant, against the possible damage to the government's security interests from disclosure." *Rahman*, 870 F. Supp. at 52.

"While the government must safeguard classified information in the interest of national security, 'courts must not be remiss in protecting a defendant's right to a full and meaningful presentation of his claim to innocence.'" *United States v. Sedaghaty*, 728 F.3d 885, 903 (9th Cir. 2013) (quoting *United States v. Fernandez*, 913 F.2d 148, 154 (4th Cir. 1990)). "[T]he defendant's right to a trial that comports with the Fifth and Sixth Amendments prevails over the governmental privilege"; if the Government refuses to produce the information the Court orders produced, the result is dismissal of the charges. *United States v. Moussaoui*, 382 F.3d 453, 474 (4th Cir. 2004). Still, the fact that defense counsel obtained security clearances does not permit unfettered access to classified discovery that a Court deems is not discoverable after conducting

the CIPA § 4 analysis. *See United States v. Libby*, 429 F. Supp. 2d 18, 24, *amended*, 429 F. Supp. 2d 46 (D.D.C. 2006) (defense team's security clearances "does not entitle them to view documents . . . that may discuss particularly sensitive issues with profound national security implications whose viewing is permitted only upon a showing that there is a 'need-to-know the information'").

A court may order the government to disclose the classified information as is, or in some other form, such as with redactions or in a summary. *See Rahman*, 870 F. Supp. 47; 18 U.S.C. APP. 3 § 6(c)(1) (authorizing "(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or (B) the substitution for such classified information of a summary of the specific classified information").

II. Analysis

A. Specific Documents

The Court has reviewed [redacted] CIA documents [redacted] that were withheld from discovery pursuant to Rule 16 and CIPA. These documents contain classified information, but are arguably discoverable under Rule 16 because they mention the Leaks. Many of them, however, are irrelevant to the charges against Schulte, as they mention the Leaks only in passing and do not go to any of the charged conduct—the theft and transmission of the Leaks to WikiLeaks.

The documents that are relevant and would be discoverable under Rule 16 clearly implicate the state-secrets privilege. The Government submitted [redacted] declarations from [redacted] high ranking officials [redacted], who assert the privilege after personal consideration. *See Aref*, 533 F.3d at 80. These documents contain highly sensitive information [redacted] such that "there is a reasonable

danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Id.* (internal quotations omitted). Specifically, disclosure of these documents [redacted] could impair the United States' ability to gather intelligence and empower the United States' adversaries. *See Rahman*, 870 F. Supp. at 50.

Most of the relevant documents are not helpful or material to Schulte. [redacted] These documents would only help the Government's case, as they show that the Leaks caused harm, and would not help Schulte. *See Rahman*, 870 F. Supp. at 52 ("[I]nculpatory material which the government does not intend to offer at trial need not be disclosed. Such information cannot conceivably help a defendant, and therefore is both unnecessary and useless to him."). They would not provide Schulte with information about how the leaked information was stolen or transmitted, possible alternative suspects, or how WikiLeaks ultimately obtained the Leaks.

Still, the Court finds that three documents are helpful or material to the defense. These documents include a report[1] by a CIA taskforce that investigated the Leaks and two documents

[1] The Government claims that this document is not discoverable under Rule 16 because it is an investigative summary drafted by the CIA. Fed. R. Crim. P. 16(a)(2) exempts from disclosure "reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." This report, however, does not appear to have been drafted in furtherance of the prosecution of this case, but rather was written [redacted] There is no indication that the report's author is an attorney or was part of the

that contain information about where the Government believes the leaked information was taken from the CIA's Local Area Network ("DevLAN"). These documents [redacted] might help Schulte advance a theory that DevLAN's vulnerabilities could have allowed someone else to have taken the leaked data. They also support the defense's theory that Schulte's behavior while an employee of the CIA was consistent with someone who was trying to help the agency address security flaws, rather than someone who was a disgruntled employee. Accordingly, these three documents go "to the innocence of the defendant *vel non*, impeach[] . . . evidence of guilt, or make[] more or less probable any fact at issue in establishing any defense to the charges." *United States v. Yunis*, 867 F.2d 617, 624 (D.C. Cir. 1989).

The Government has proposed redactions or summaries of these documents, which the Court has reviewed and concludes provide Schulte "with substantially the same ability to make their defenses as would disclosure of the specific classified information."[2] *United States v. Fawwaz*, S7 98 Crim. 1023(LAK), 2013 WL 5429226, at *1 (S.D.N.Y. Sept. 24, 2013). The redactions and summaries accurately represent the original documents without obscuring any of the information that is helpful to Schulte, while minimizing the amount of irrelevant classified

---

investigation team for the present case. [redacted] This is not the type of government report that is usually excluded from discovery pursuant to Rule 16(a)(2). *Compare United States v. Nashash*, No. 12 CR 00778 PAC, 2014 WL 169743, at *1 (S.D.N.Y. Jan. 15, 2014) (discovery request—for information about DEA's classification decision for certain controlled substances and background information about how tests were performed on substances seized from Defendants –dealt with "the predicate for the investigation"; information sought was thus not exempt from discovery under Rule 16(a)(2)), *with United States v. Ceballo*, No. 03 CR. 283 (SWK), 2003 WL 21961123, at *1 (S.D.N.Y. Aug. 18, 2003) (quashing subpoena of NYPD investigatory files concerning arrest of defendant).

[2] The Government maintains that these documents are not discoverable and/or are not helpful to the Defendant. The Government also argues that the information contained in these documents is cumulative, as the same information has already been produced to Defendant.

information that could be disclosed. This approach strikes the right balance between protecting the flow of information against Schulte's right to prepare his defense. *See Mostafa*, 992 F. Supp. 2d at 338; *see generally* 18 U.S.C. APP. 3 § 4 (noting that the Court may authorize the Government to "substitute a summary" for classified information). The Government is directed to produce these three documents in their redacted or summarized forms.

B. Email Communications

The Government conducted a review of every email and chat sent by or to Schulte, but produced only those documents it viewed as relevant to the charged conduct, with redactions to certain classified information. Defense counsel has requested Schulte's entire email account, and the Government has indicated that it is willing to supplement its production by producing all of Schulte's sent email communications during the relevant time period. Relevant communications have already been produced to satisfy the obligations of Rule 16, and the Government's proposed compromise provides Schulte with further access to emails he drafted so that he may craft his defense, while protecting against the disclosure of irrelevant classified information, such as information that could identify undercover CIA officers, from emails sent to Schulte. The Government's proposed compromise comports with its obligations under Rule 16 and CIPA.[3]

C. Forensic Discovery

The Court now turns to the complex topic of forensic discovery. At trial, the Government must establish that Schulte accessed and stole classified information from DevLAN. The Government will need to explain to a jury how the CIA's systems were structured, demonstrate what Schulte's activities were on the CIA's system that indicate he stole the leaked

[3] Other identifying information for CIA officers and administrative information about the CIA was also properly withheld. Relevant identifying information has already been produced in classified discovery. Any further information is either irrelevant or cumulative.

data, and show that other individuals did not steal the leaked data. Accordingly, forensic evidence, such as log files, metadata, backup data, and removable storage devices will comprise a large part of the evidence in support of the Government's case. Schulte has requested that the Government provide him with a complete forensic copy of the Schulte Workstation and DevLAN, so that his cleared expert can conduct a comprehensive forensic analysis to rebut the Government's forensic case and show that individuals other than Schulte within or outside the CIA could have or did steal the leaked data.

The Government states that the only forensic evidence that is consistent with the removal of the leaked information is on the Schulte Workstation, and uses this conclusion to justify turning over only some data from Schulte's Workstation—the data that supports the Government's theory of its case. The Government also did not produce a complete forensic copy of DevLAN, which could show other users' activity and potential vulnerabilities of the system, if any existed. The Court reviewed the Government's methodology for identifying and excluding irrelevant and/or classified material, which the Government asserts protected CIA equities while still providing the defense with access to relevant information. The Government claims that the CIA's procedure for identifying and deleting irrelevant documents was reasonable and necessary to facilitate production of voluminous discovery, but that to the extent Schulte articulated a justifiable need for additional material, the Government would work with the defense and the CIA to produce that material. This approach is generally satisfactory.

In the interest of putting ourselves in the shoes of defense counsel, who cannot read the CIPA § 4 brief, and acting with a view of Schulte's interests, *Amawi*, 695 F.3d at 471, the Court recognizes that the form of the Government's initial production of forensic discovery may create difficulties for Schulte's cleared forensic expert to conduct his investigation to aid in Schulte's

defense. It may be the case that more disclosure of the Schulte Workstation and DevLAN would be relevant and helpful to Schulte and discoverable under Rule 16. The primary evidence tying Schulte to the theft of the leaked data is forensic in nature, and centers on the Schulte Workstation and DevLAN. It is not Schulte's burden to establish who took the data; rather, the government must establish beyond a reasonable doubt what Schulte did. Indeed, Schulte has no burden. Still, the defense may conduct its own investigation into whether anyone other than Schulte could have stolen the data. *See California v. Trombetta*, 467 U.S. 479 (1984) (Criminal defendants must "be afforded a meaningful opportunity to present a complete defense. To safeguard that right, the Court has developed what might loosely be called the area of constitutionally guaranteed access to evidence."). Under Rule 16, the Government must produce not only the evidence that it plans to use in its own case-in-chief, but also the data that is material to Schulte's defense. *See* Fed. R. Crim. P. 16(a)(1)(E).

Without a deeper review of DevLAN, Schulte may be hindered in rebutting the forensic evidence which is the basis for the Government's case. On the other hand, the Government must introduce at trial voluminous forensic evidence to establish Schulte's guilt. All of that evidence will be subject to vigorous cross examination. The complex measures that are currently in place to ensure that the classified discovery in this case is reviewed in a secure facility by cleared attorneys and Schulte himself should alleviate some concerns about Schulte's trial preparation.

Of course, the Court is mindful of the immense size of the full universe of forensic data and of the serious national security concerns inherent to producing the totality of Schulte's requests. The Government put in a great deal of planning and effort in collecting, reviewing, and producing what might be an unprecedented volume of classified discovery to Schulte. Complete forensic copies of the Schulte Workstation and DevLAN would contain a tremendous amount of

classified information. [redacted] Schulte has been accused of leaking information he obtained from his employment at the CIA both before he was arrested and from his cell at MCC after his arrest.[4] Granting him unfettered access to the Schulte Workstation and DevLAN would gut the entire rationale behind CIPA. There is clearly "a reasonable danger that disclosure of this evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Aref*, 533 F.3d at 80.[5]

Both sides have strong interests. The Government's approach strikes the Court as more reasonable than Schulte's, given the purpose of CIPA, the strong national security interests that are implicated by the data he requests, and the vast scope of Schulte's demands. Schulte is not entitled to unfettered access to the Schulte Workstation and DevLAN. Still, the Court will leave open the possibility of ordering production of forensic data beyond what supports the Government's own theory of the case if Schulte submits a more tailored request and provides good reason for further forensic discovery in a motion to compel. In this context, it would also be helpful, for example, if Schulte would communicate his thinking of how others are responsible for the theft.

If the parties can resolve forensic discovery issues by meeting and conferring in light of this opinion, all the better. The Government and Schulte have been cooperating to resolve

---

[4] Schulte has filed a motion to suppress the evidence seized from his cell at MCC. (Dkt. 97.)

[5] The declarations submitted by the Government describe the process and justification for deletions of certain forensic data, in accordance with *Aref*.

discovery disputes already.[6] This collaboration should continue with regard to the Schulte Workstation and DevLAN.

CONCLUSION

The Government's motion is granted in part. The CIPA § 4 submissions will be sealed. The CIA is directed to complete classification review of this Order within 14 days. This Order will be considered presumptively classified until then. A public Order will be published with necessary redactions upon completion of the classification review.

Dated: New York, New York
July 22, 2019

SO ORDERED

PAUL A. CROTTY
United States District Judge

[6] The Government has offered to produce additional source code that is relevant to the tools Schulte worked on at the CIA, if a need is articulated. The Government has also offered to produce further log files that Schulte's expert needs to conduct a forensic investigation. In addition, the parties' forensic experts have met, so that the Government's expert can articulate what forensic evidence does or does not exist, and so that Schulte's expert can explain what further discovery Schulte needs to conduct an investigation so that he may present his own forensic case to the jury that he could not have, or someone else could have, stolen the leaked data.